NHTSA-2008-0019

February 25, 2008

The Honorable Nicole R. Nason
Administrator
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE.,
West Building, 4th Floor,
Washington, DC 20590

Dear Nicole R. Nason:

[Docket No. NHTSA-2008-0004] RIN 21`27-AK 12 or subsequently NHTSA-2006-25666.

RE: Petition for Reconsideration to 49 CFR Part 563 Event Data Recorders – Response to Petitions for Reconsideration as published in the *Federal Register* / Vol. 73, No. 9 / Monday, January 14, 2008 / Rules and Regulations.

Specifically, I Petition for Remand due to factual errors in the Agency response to the following section:

> *H. Public Privacy and Consumer Notification of EDRs*
>
> 1. Whether NHTSA Should Require a Mechanical Lockout on EDRs.
>
> Mr. Thomas Kowalick petitioned NHTSA to require a mechanical lockout on the on-board diagnostic (OBD2) port [28] for the sole use/control of the owner or operator of the vehicle equipped with an EDR. Mr. Kowalick argued that it is possible to protect consumer privacy rights by use of a mechanical lockout system on this port, which is used to download EDR data. In a March 1, 2007 meeting with NHTSA, Mr. Kowalick expressed an additional concern that aftermarket devices are being developed to erase or tamper with EDR data.[29] **He noted that the preamble to the final rule stated that if tampering became apparent, NHTSA would reconsider its position on this issue.**
>
> *Agency response:* We are denying this petition. Mr. Kowalick provided information that devices may exist to erase or tamper with EDR data, but he did not provide information that they were actually being used. There are several other ways that EDR tampering will be prevented. First, the EDR download port is installed inside the vehicle, on which the door locks act as a first line of defense to prevent access to the data port. Second, if the vehicle glazing is missing, either due to an accident or forceful entry (assuming a person wants to tamper with someone else's EDR data), the vehicle key is needed to power the vehicle to access the EDR data through the diagnostic port. And third, the final rule requires that event data from crashes in which an air bag has been deployed must be locked and cannot be overwritten. **As stated in the final rule, the agency may revisit the issue if EDR tampering indeed becomes a problem.**
>
> 28 *See* 61 FR 40940. The OBD2 port standard specifies the type of diagnostic connector and its output pin locations used for monitoring vehicle parameters measured by the on-board computer(s) such as emissions controls. It is typically located on the driver's side of the passenger compartment near the center console.
> 29 Docket No. NHTSA–2006–25666–457.

I petition NHTSA for remand based on evidence of tampering. Thus, I am providing information to persuade NHTSA that conditions have changed meaningfully since the Agency's original determination— specifically with current tampering of EDR data and odometer readings.

Definition of Tampering

"Tampering" means to modify, remove, render inoperative, cause to be removed, or make less operative any device or element design installed on a motor vehicle or motor vehicle power-train, chassis or body components which results in altering federal motor vehicle safety standards (FMVSS).

Providing the Agency Evidence of Tampering Devices

Docket NHTSA-2006-25666-457 clearly establishes that numerous devices exist to reset air bags, erase crash data and/or modify odometer readings. In that docket I cited 29 products from 23 companies advertised with capabilities to alter or omit crash data by plugging an inexpensive software/hardware device into the vehicle OBD port.

Providing the Agency Evidence of Tampering Services

Here are four (4) examples as advertised online (last visited 2/27/08).

http://www.talktomycar.co.uk/index.htm
http://www.airbagcrash.com/
http://www.tachosoft.com/_airbag.htm
http://www.autodiag.ru/airbagaudivwen.html

NHTSA Initiatives Call for Increased Measures but Fail to Provide an Effective Counter-Measure

The Agency maintains an Office of Odometer Fraud Investigation with a web site at http://www.nhtsa.dot.gov/portal/site/nhtsa/menuitem.893c19c9fb974f825c420087dba046a0/

This site provides the following assessment:

> Odometer tampering continues to be a serious crime and consumer fraud issue. In 2002, NHTSA determined this crime allows more than 450,000 vehicles to be sold each year with false odometer readings, milking American car buyers out of more than $1 billion annually. From 2002 to 2005, we have seen a definite escalation of odometer fraud. New car prices, coupled with the increased demand for late-model, low-mileage used cars, has made odometer fraud more profitable than ever. Strong enforcement of the federal and state odometer laws, i.e., prosecutions with stiff sentences, appears to be the most effective deterrent.

The Nature of Odometer Fraud According to the U.S. Department of Justice (USDOJ)

> Odometer fraud is a pernicious crime that robs thousands of dollars from each victim it touches. See, e.g., *United States v. Whitlow, 979 F.2d 1008, 1012 (5th Cir. 1992)* (under sentencing guidelines, court affirmed estimate that consumers lost $4,000 per vehicle). The television news magazine 60 Minutes once characterized it as the largest consumer fraud in America. Victims of this fraud are commonly the least able to afford it, since buyers of used cars include large numbers of low income people. In addition, consumers generally are unaware of being victimized.
>
> Odometer-tampering involves several interrelated activities. Late-model, high-mileage vehicles are purchased at a low price. The vehicles are "reconditioned" or "detailed" to remove many outward appearances of long use. Finally, odometers are reset, typically removing more than 40,000 miles.
>
> In addition to the cosmetic "reconditioning" of the car, the odometer tamperer "reconditions" paperwork. Automobile titles include a declaration of mileage statement to be completed when ownership is transferred. To hide the actual mileage that is declared on the title when the car is sold to an odometer tamperer, the tamperer must take steps to conceal this information. These steps vary from simple

alteration of mileage figures, to creating transfers to fictitious "straw" dealerships to make it unclear who was responsible for the odometer rollback and title alteration. Alternatively, the odometer tamperers frequently destroy original title documents indicating high-mileage, and obtain duplicate certificates of title from state motor vehicle departments, upon which the false, lower mileage figures are entered.

Whatever method is used, the result is the same. The odometer tamperer possesses an altered, forged, or replacement title document (which is a security under federal law) containing a false low-mileage reading. This title is used to sell the car, for several thousand dollars above its actual value, to a purchaser who is deceived regarding the vehicle's remaining useful life by the altered odometer, by the vehicle's outward appearance, and by the counterfeit, low-mileage title and odometer statement. [1]

Rationale for this Petition for Reconsideration stressing that the Agency has the authority and responsibility to act in a timely manner to correct clearly erroneous errors:

1. The Agency already acknowledges tampering devices exist to erase crash data and alter odometers, and promises ***if tampering became apparent it would reconsider its position on this issue.*** This petition provides evidence of tampering.

2. The Agency's EDR rulemaking ***is inadequate to protect owner/operators*** of an estimated sixty (60) million vehicles that currently utilize event data recorder (EDR) technologies as proven by the fact that EDR data is widely used in civil and criminal cases.[2] Even though the majority of vehicle owners are unaware of the presence of these "black boxes" in their vehicle, criminal prosecutors and personal injury attorneys are obtaining the data contained in these "black boxes" from owners' vehicles and using the data contained within to charge drivers with crimes or hold them liable for damages in personal injury lawsuits. Numerous unsuspecting vehicle operators have been convicted, sentenced and jailed based, in part, on the black box data extracted from their vehicles. [3]

3. Door locks ***do not serve as an adequate defense to prevent access*** to the diagnostic link connector (DLC) data port. Following a crash numerous personnel including first responders, law enforcement and other third parties such as vehicle towing and insurance adjusters have access to the interior of the vehicle and thus to the diagnostic link connector (DLC) port. Therefore, an open port is always subject to tampering. (see figure 1).

4. Furthermore, ***a vehicle key is NOT NEEDED to access the EDR data*** since the Agency is fully aware that there are alternative methods to provide power via the fuse box. [4] The Agency also understands future vehicles will include keyless ignitions.

---

[1] See http://www.usdoj.gov/civil/ocl/monograph/odom.htm (Last visited 2/25/2008)

[2] EDR case law online at http://www.collisionsafety.net/cdrcaselaw.htm (Last visited 2/25/2008).

[3] See http://lemonfax.com/industry_secrets.html (Last visited 2//25/2008).

[4] The Agency participated in a National Academies of Science / Transportation Research Board (NSA/TRB) National Cooperative Highway Research *Project 17-24 Use of Event Data Recorder (EDR) Technology for Highway Crash Analysis* study in which a section (4) was devoted to EDR Data Retrieval Methods and Issues: Section 4.2.2 specifically outlines NHTSA experience with EDR Data Retrieval; and Section 4.2.3 specifically details Interviews with NASS Field Accident Investigators. Thus, the Agency is well versed on alternative methods of accessing data without a vehicle key. The full report is available online at: www-nrd.nhtsa.dot.gov/edr-site/uploads/TRB_NCHRP_Project_17-24.pdf - Other EDR Downloading Concerns. Assuming that the accident investigation teams are able to download

5. Finally, although the Agency cites that event data from crashes in which an air bag has been deployed must be locked and cannot be overwritten ***the Agency failed to define the term "lock."*** [5] ***which permits a high likelihood of confusion and misunderstanding.***

In conclusion, although NASS investigation teams may be properly collecting EDR crash data the Agency cannot determine – one way or the other – if or when motor vehicle event data recorders or odometers are tampered with by other parties, therefore, calling into question the validity of the data gathered or a rationale for lack of data (once erased). To remedy this situation the Agency should quickly correct clearly erroneous factual errors and mandate a mechanical lockout on the diagnostic link connector (DLC) for vehicles that include EDRs or provide access to odometer settings via the DLC. This is an immediate and urgent issue. A simple OEM or aftermarket lockout product is readily feasible. Vehicle OEMs would welcome this means of protecting data and preventing re-engineering. The estimated cost per vehicle would be approximately two dollars. This would be a small price for providing consumer protection towards assuring consumer acceptance of these emerging life saving technologies. I welcome the opportunity to provide additional information to the Agency on this issue. I also volunteer to provide a demonstration of how to secure the ODB DLC port without interfering with scheduled maintenance, inspection or repair of the vehicle as required. **Thus, based on the evidence presented to the Agency there are no substantive reasons for denial of this timely petition.**

Thomas M. Kowalick

Sincerely,

Thomas M. Kowalick
305 South Glenwood Trail
Southern Pines
North Carolina, 28387

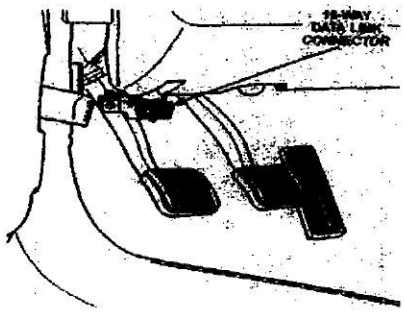

Figure 1

---

the EDR from the OBD-II port, they need to obtain the vehicles keys to operate the ignition. Contrary to overall NHTSA findings, the Ocean County team reported that obtaining the vehicles keys was not a problem, making this method of download a simple process when OBD-II download functions correctly. GM Experience with EDR Data Retrieval: The research team followed up these interviews with a phone interview with a subject EDR expert at GM [Floyd, 2003]. GM reports significantly higher success rates at downloading their EDRs through the OBD-II connector. GM uses a technique of externally powering the airbag control module through the fuse box when the car has lost power or no key is available. GM reports that this technique works unless there is significant intrusion or unless the OBD-II connection has been grounded. It should be noted that this technique is not however part of the currently recommended practice when using the Vetronix CDR tool. Using techniques such as these, however, GM estimates that their EDRs can be downloaded through the OBD-II connector 80% of the time. Only an estimated 20% of the attempted downloads require direct connection with cables. In an estimated 5% of all cases, no data can be recovered for reasons including water immersion, fire, or severe crash damage.

[5] During this same EDR rulemaking in response to a petition from AORC the Agency stated "If we allowed the EDR to be erased by external means, it could encourage development of tools to erase EDR data potentially beneficial to our programs, and would make it difficult to ensure that this feature was not being misused. Although the final rule did not define the term "locked," we consider it to mean to protect EDR data from changes or deletion. This would include by external means." (note- these tools are being used!)